Cyber Security and Information Assurance (CSIA)

NITRD Agencies: NSF, OSD and DoD Service research organizations, NIH, DARPA, NSA, NASA, NIST
Other Participants: CIA, DHS, DOE (LLNL), DOJ, DOT, DTO, FAA, FBI, State, Treasury, TSWG

CSIA focuses on research and advanced development to prevent, resist, detect, respond to, and/or recover from actions that compromise or threaten to compromise the availability, integrity, or confidentiality of computer-based systems. These systems provide both the basic infrastructure and advanced communications in every sector of the economy, including critical infrastructures such as power grids, emergency communications systems, financial systems, and air-traffic-control networks. These systems also support national defense, national and homeland security, and other vital Federal missions, and themselves constitute critical elements of the IT infrastructure. Broad areas of concern include Internet and network security; confidentiality, availability, and integrity of information and computer-based systems; new approaches to achieving hardware and software security; testing and assessment of computer-based systems security; and reconstitution and recovery of computer-based systems and data.

Incorporation of the CSIA Program Component Area and the CSIA Interagency Working Group (IWG) into the NITRD Program

In August 2005, the NSTC chartered the Cyber Security and Information Assurance (CSIA) IWG. This IWG succeeds the IWG on Critical Information Infrastructure Protection (CIIP), which had been chartered in August 2003 and reported to the Subcommittee on Infrastructure of the NSTC's Committee on Homeland and National Security. The CSIA IWG reports jointly to the Subcommittee on Infrastructure and the NITRD Subcommittee. This change facilitates better integration of CSIA R&D with NITRD activities and reflects the broader impact of cyber security and information assurance beyond critical information infrastructure protection.

The first steps in integrating CSIA R&D into NITRD activities involve incorporating the budget associated with the CSIA PCA and the coordination by the CSIA IWG into the NITRD Program, and completing and releasing the Federal Plan for CSIA R&D (described below). Future steps will include roadmapping CSIA R&D and adjusting the activities in NITRD PCAs in light of the Program's expanded scope. Selected areas requiring cross-PCA coordination are described below.

President's 2007 Request

Strategic Priorities Underlying This Request

Fundamental and applied research for CSIA: New knowledge, technologies, and tools to achieve significantly improved security for the computer-based systems that support national defense, national and homeland security, economic competitiveness, and other national priorities. Key research areas include:

– **Network security:** New communications protocols, especially for wireless networks and mobile ad hoc networks, required to effectively secure networks and the data that travel over them (with LSN)

– **Dependable systems:** Systems with characteristics that include fault tolerance, reliability, safety, and security (with HCSS)

– **Situational awareness and response:** Data fusion and forensics, security visualization, and security management

– **Secure distributed systems:** Ability to function as network-centric multi-domain enterprise with ubiquitous secure collaboration

Infrastructure protection: Computer-based systems that function as intended, even in the face of cyber attack, and that are able to process, store, and communicate sensitive information according to specified security policies (with HCSS)

Infrastructure for R&D: Testbeds, tools, platforms, standards, and data collection and sharing to enable academic, industry, and government researchers to effectively conduct CSIA R&D

Industry outreach and technology transfer: Effective transition and diffusion of R&D results into mainstream products and services and improved practices; increased coordinated industry outreach and technology transfer to aid timely transition of existing and newly created CSIA R&D to practice, including standards, guidelines, metrics, benchmarks, and best practices

Highlights of Request

Cyber Trust: Academic research in foundations, network security, secure systems software, security of information systems – NSF, DARPA

Testbeds: Development, testing, and evaluation of testbeds for the DETER, EMIST, and GENI projects – NSF, DHS

Datasets: Complete secure, trusted data-sharing infrastructure and initial data collection and sharing – NIST, NSF, DHS

Internet infrastructure security: Domain Name System (DNS) security roadmap, testing, guidance, and routing protocol security – NIST, DHS

Planning and Coordination Supporting Request

Federal Plan for Cyber Security and Information Assurance Research and Development

The CSIA IWG was charged with developing an interagency Federal Plan for CSIA R&D. This forthcoming document, which represents a collaborative effort by the CSIA IWG members, provides a baseline framework for coordinated, multiagency CSIA R&D. The Plan is currently in final clearance.

The Federal Plan resulted from a process in which CSIA R&D needs were identified, analyzed, and prioritized. Part I of the Federal Plan includes sections on:

- Technology Trends
- The Federal Role
- Types of Threats and Threat Agents
- Threat and Vulnerability Trends
- Recent Calls for CSIA R&D
- Strategic Federal Objectives
- R&D Technical and Funding Priorities
- Top Technical and Funding Priorities
- Findings and Recommendations

Part II of the Plan contains commentaries on technical topics. Each commentary includes a definition of the topic and discussions of its importance, the state of the art, and capability gaps requiring R&D. The technical topics are grouped in the following eight broad R&D categories identified in the CSIA IWG's analysis: functional cyber security; securing the infrastructure; domain-specific security; cyber security characterization and assessment; foundations for cyber security; enabling technologies for CSIA R&D; advanced and next-generation systems and architecture for cyber security; and social dimensions of cyber security.

Other Interagency Planning and Coordination Activities

Roadmapping: Develop an initial roadmap that provides a timeline for activities needed to implement the Federal Plan for CSIA R&D – CSIA IWG

Cyber security R&D:

– System resilience: Intrusion tolerance, self-regenerating systems, dynamic quarantine of worms, detection and containment of malicious code – DARPA, DoD (AFRL)

– Adaptive quarantine: Development of adaptive quarantine to prevent and preempt active, passive, novel insider and outsider cyber attacks against safety-critical and mission support networks and systems enterprise-wide – DTO, FAA

– Intrusion detection: Intrusion detection and monitoring, cyber attack detection, traceback, and attribution – NSA, DoD (AFRL), DTO

– Countermeasures: Flash ROM countermeasures tool and technologies that address identity theft and fraud detection – TSWG, FBI

– Power grid: Trustworthy cyber infrastructure for the power grid – DHS, NSF, DOE

– Election systems: Trustworthy election systems – NIST, NSF

Grants and proposals: Collaborate/coordinate on solicitations and evaluations – DARPA, NSA, NSF, DHS, DTO

National Plan for Research and Development in Support of Critical Infrastructure Protection: Provide input to the NSTC Subcommittee on Infrastructure on cyber aspects of critical infrastructure protection – CSIA IWG

INFOSEC Research Council *Hard Problem List*: Support the preparation of the *Hard Problem List* released in November 2005 – Multiple agencies

Cyber Security: A Crisis of Prioritization: Respond to the PITAC report's recommendations – CSIA IWG

Improving Cybersecurity Research in the United States*:* Continue support for National Academies study – DARPA, NIST, NSF

Additional 2006 and 2007 Activities by Agency

NSF: Team for Research in Ubiquitous Secure Technology (TRUST) to transform the ability of organizations to design, build, and operate trustworthy information systems for critical infrastructures; industry/university cooperative research centers in information protection, computer systems, and identification technology; Scholarship for Service program; advanced technology education

OSD (ODDR&E): Through the High Performance Computing Modernization Program, adapt network intrusion detection and analysis tools to improve collective analysis of multiple sensor inputs and to support IPv6

DARPA: R&D in security-aware systems

NSA: Cryptography, cryptographic infrastructure; high-speed security solutions, security-enhanced operating environment, secure wireless multimedia; authentication, privilege management; attack-sensing warning and response, insider threat, and network dynamics

NASA: Next-generation HEC perimeter protection architecture and system for Columbia supercomputer (a possible model for HEC system security at other agencies), including a new security approach for network-intensive applications and the coupling of two-factor authentication to unattended file transfers

NIST: FISMA standards and guidelines; state and local municipality outreach; secure OS and application configuration specifications, identity management, smart-card interoperability specifications, conformance testing; cryptographic standards, guidelines, tool kit, module validation; PDA forensics guidelines and computer forensics tool effectiveness testing; access control, policy management modeling and prototypes; technology-specific security guidelines (e.g., RFID, Web services, Wi-Max); remote authentication methods; wireless/PDA security protocols, mechanisms, and seamless/secure mobility; automated combinatorial testing; National Vulnerability Database

DHS: Vulnerability prevention, discovery, and remediation; cyber security assessment; security and trustworthiness for critical infrastructure protection; wireless security; network attack forensics; technologies to defend against identity theft; continued support for the Process Control Systems Forum

DOE (LLNL): R&D on extracting novel forensic information from hostile scan data and developing statistical and trending analysis for cooperative protection program data

DOJ: Common solutions to security requirements to achieve cost efficiency through broad implementation; incident response and situational awareness

DOT: Secure aircraft data networks and applications; security testing and penetration testing methods; biometrics and access control security for aircraft cockpits and aircraft; risk assessment methods; credentialing; advanced wireless technologies

FAA: Rapid quarantine capability; test biometrics single sign-on; test behavior-based security; enterprise architecture based on the DoD architecture framework; information systems security architecture as enclave with demilitarized zone; integrity and confidentiality lab to test wireless systems security; validate Web data mining that uses concept chain graphs to find vulnerabilities

FBI: Advanced visualization concepts for analyzing various data media types; state-of-the-art integrated analytical tools that support law enforcement investigations; cyber-capabilities-driven enterprise architecture as a business and management tool

TSWG: Secure ground-to-air data communications; automate cyber assessment at the Nuclear Regulatory Commission; develop commercially viable cyber security testing; establish cyber security training center; assess state of the art in infrastructure modeling capabilities